CLAIMS

1. A method for authenticating a terminal in a communication system, the terminal comprising identification means for applying authentication functions to input data to form response data, and the communication system being arranged to utilise a first authentication protocol for authentication of the terminal, wherein an authentication functionality and the terminal share challenge data, the terminal forms response data and a first key by applying the authentication functions to the challenge data by means of the identification means, and returns the response data to the authentication functionality, and the authentication functionality authenticates the terminal by means of the response data and can apply an authentication function to the challenge data to duplicate the first key; the method comprising;

executing a second authentication protocol wherein the terminal authenticates the identity of a network entity and the terminal and the network entity share a second key for use in securing subsequent communications between the terminal and the network entity;

and subsequently executing a third authentication protocol by the steps of:

sharing challenge data between the network entity and the terminal;

forming at the terminal test data by at least applying one of the authentication functions to the challenge data by means of the identification means;

transmitting a message comprising terminal authentication data, from the terminal to the network entity;

and determining based on the terminal authentication data whether to provide the terminal with access to a service;

wherein in the determining step the terminal is provided with access to the service only if the terminal authentication data equals a predetermined function of at least the test data and the second key.

2. A method as claimed in claim 1, wherein the method comprises:

forming the test data by applying the authentication function to the challenge data at the authentication functionality; and

transmitting the test data from the authentication functionality to the network entity;

and wherein the determining step comprises forming network authentication data by applying the predetermined function to the test data and the key at the network entity; and in the determining step the terminal is provided with access to the service only if the terminal authentication data equals the network authentication data.

3. A method as claimed in claim 1, wherein the method comprises:

transmitting the second key from the network entity to the authentication functionality;

forming the test data by applying the authentication function to the challenge data at the authentication functionality; and

forming network authentication data by applying the predetermined function to the test data and the key at the authentication functionality.

4. A method as claimed in claim 3, comprising:

transmitting the terminal authentication data from the network entity to the authentication functionality;

transmitting from the authentication functionality to the network entity an indication of whether the terminal authentication data equals the network authentication data;

and wherein in the determining step the terminal is provided with access to the service only if the indication is that the terminal authentication data equals the network authentication data.

5. A method as claimed in claim 3, comprising:

transmitting the network authentication data from the authentication functionality to the network entity;

and wherein in the determining step the terminal is provided with access to the service only if the indication is that the terminal authentication data equals the network authentication data.

6. A method as claimed in any preceding claim, wherein the terminal authentication data is formed as a cryptographic checksum

7. A method as claimed in any preceding claim, wherein the network entity is co-located with the authentication functionality.

8. A method as claimed in any preceding claim, wherein authentication means is an identity module of the terminal.

9. A method as claimed in claim 8, wherein the identity module is user-removable from the terminal.

10. A method as claimed in claim 8 or 9, wherein the identity module is a SIM or a USIM.

11. A method as claimed in any preceding claim, wherein the first authentication protocol is the AKA protocol or any protocol of the EAP family.

12. A method as claimed in claim 11 as dependent on any of claims 2 to 6, wherein the test data includes one or both of the AKA IK value or the AKA CK value.

13. A method as claimed in any preceding claim, wherein the authentication means stores a code and the authentication function comprises applying a cryptographic transformation to the code and the input data.

14. A method as claimed in any preceding claim, wherein the second authentication protocol is the PIC, the PEAP protocol or the EAP-TTLS protocol.

15. A method as claimed in any preceding claim, wherein the challenge data and the response data are formed according to the EAP protocol.

16. A method as claimed in any preceding claim, wherein the said message is a dedicated authentication message.

17. A method as claimed in any preceding claim, wherein the predetermined function is used for derivation of a session key to be used for encryption and/or authentication of communications between the terminal and the network entity.

18. A communication system comprising identification means for applying authentication functions to input data to form response data, and the communication system being arranged to utilise a first authentication protocol for authentication of the terminal, wherein an authentication functionality and the terminal share challenge data, the terminal forms response data and a first key by applying the authentication functions to the challenge data by means of the identification means, and returns the response data to the authentication functionality, and the authentication functionality authenticates the terminal by means of the response data and can apply an authentication function to the challenge data to duplicate the first key; the system being arranged to perform an authentication method comprising the steps of:

executing a second authentication protocol wherein the terminal authenticates the identity of a network entity and the terminal and the network entity share a second key for use in securing subsequent communications between the terminal and the network entity;

and subsequently executing a third authentication protocol by the steps of:

sharing challenge data between the network entity and the terminal;

forming at the terminal test data by at least applying one of the authentication functions to the challenge data by means of the identification means;

transmitting a message comprising terminal authentication data, from the terminal to the network entity;

and determining based on the terminal authentication data whether to provide the terminal with access to a service;

wherein in the determining step the terminal is provided with access to the service only if the terminal authentication data is consistent with the network authentication

data computed as a predetermined function of at least the test data and the second key.

19. A communication system comprising a terminal, a network entity and an authentication functionality, the terminal comprising identification means for applying an authentication function to input data to form response data, and the communication system being arranged to utilise a first authentication protocol wherein the terminal authenticates the identity of a network entity and the terminal and the network entity share a key for use in securing subsequent communications between the terminal and the network entity; and the communication system being arranged to perform an authentication method comprising the steps of: executing a second authentication protocol for authentication of the terminal, wherein an authentication functionality supplies challenge data to the terminal, the terminal forms response data and test data by applying the authentication function to the challenge data by means of the identification means, and returns the response data to the authentication functionality, and the authentication functionality authenticates the terminal by means of the response data; and subsequently executing a third linking protocol by the steps of forming at the terminal secret session keys by at least applying a predetermined function to the secret test data by means of the shared key established in the first protocol; forming at the network entity secret session keys by at least applying a predetermined function to the secret test data by means of the shared key established in the first protocol; wherein in the secret session keys are used to secure the subsequent communication between the terminal and some network element.

20. A an authentication method for use in a communication system comprising a terminal, a network entity and an authentication functionality, the terminal comprising identification means for applying an authentication function to input data to form response data, and the communication system being arranged to utilise a first authentication protocol wherein the terminal authenticates the identity of a network entity and the terminal and the network entity share a key for use in securing subsequent communications between the terminal and the network entity; and the

authentication method comprising the steps of: executing a second authentication protocol for authentication of the terminal, wherein an authentication functionality supplies challenge data to the terminal, the terminal forms response data and test data by applying the authentication function to the challenge data by means of the identification means, and returns the response data to the authentication functionality, and the authentication functionality authenticates the terminal by means of the response data; and subsequently executing a third linking protocol by the steps of forming at the terminal secret session keys by at least applying a predetermined function to the secret test data by means of the shared key established in the first protocol; forming at the network entity secret session keys by at least applying a predetermined function to the secret test data by means of the shared key established in the first protocol; wherein in the secret session keys are used to secure the subsequent communication between the terminal and some network element.

21. A method for authenticating a terminal in a communication system, substantially as herein described with reference to the figures 7 and 8 of the accompanying drawings.

22. A communication system substantially as herein described with reference to figures 7 and 8 of the accompanying drawings.